UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

KRISTEN EYESTER, individually and on behalf of all others similarly situated, Plaintiff, v. **NUANCE COMMUNICATIONS, INC.,** Defendant.	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Kristen Eyester ("Plaintiff"), individually and on behalf of herself and all others similarly situated, allege the following against Nuance Communications, Inc. ("Nuance" or "Defendant"). The following allegations are based upon Plaintiff's personal knowledge with respect to herself and her own acts, and on information and belief as to all other matters.

I. INTRODUCTION

1. Plaintiff and Class Members bring this class action against Nuance for its failure to properly secure and safeguard Plaintiff's and similarly situated individuals' personally identifiable information ("PII") and protected health information ("PHI")—as defined by the Health Insurance Portability and Accountability Act ("HIPAA")—including but not limited to names; demographic information (including address, phone number, email address, gender, date of birth); relatives' names; power of attorneys' names; health insurance numbers; dates of service; medical facilities; practitioners' names; diagnostic study identifiers such as accession number and study UID; clinical information such as treatments provided, medication information, diagnoses, diagnostic imaging reports; and patient identifiers such as medical record numbers.

2. Nuance is a global provider of conversational artificial intelligence and cloud-based ambient clinical intelligence for healthcare providers. Through Nuance's contracts with healthcare providers, including WakeMed Health & Hospitals, Nuance cumulatively possesses and stores the PII and PHI of hundreds of millions of people in its databases.

3. This class action is brought on behalf of all citizens of all states in the United States who are the victims of a targeted cyberattack on Nuance Communications, Inc. that occurred on or before May 28, 2023 ("the Data Breach").

4. On or before May 28, 2023, Nuance allowed a cyber attacker to access and obtain the PII and PHI of Plaintiff and Class Members.

5. Over one month later, on or around July 10, 2023, Nuance confirmed that individuals' PII and PHI was exposed in the Data Breach.

6. Over three months after the Data Breach, on or around September 15, 2023, Nuance began filing Notice templates with state attorneys general. These Notice templates, however, failed to provide basic details concerning the Data Breach, including, but not limited to, how unauthorized parties accessed the Class Members' records, whether the information was encrypted or otherwise protected, or whether the breach was a system-wide breach. The Notice also failed to provide details on how many people were affected by the Data Breach.

7. Nuance knowingly collected individuals' PII and PHI in confidence, and has a resulting duty to secure, maintain, protect, and safeguard that PII and PHI against unauthorized access and disclosure through reasonable and adequate security measures.

8. PHI is considered "the most confidential and valuable type of [PII] . . . irrevocable once breached."[1]

9. As a result of the Data Breach, Plaintiff and Class Members suffered actual, ascertainable losses, including, but not limited to, identity theft/email fraud, the loss of value of their private and confidential information, the loss of the benefit of their contractual bargain with Nuance, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiff and Class Members entrusted their Private Information to Nuance, its officials, and agents. That Private Information was subsequently compromised, unlawfully accessed, and stolen due to the Data Breach.

11. Plaintiff brings this class action lawsuit on behalf of herself and all others similarly situated to address Nuance's inadequate safeguarding of Plaintiff's and Class Members' Private Information, for failing to provide adequate notice to Plaintiff and other Class Members of the unauthorized access to their Private Information by a cyber attacker, and for failing to provide adequate notice of precisely what information was accessed and stolen.

[1] Junyuan Ke, et al., *My Data or My Health? Heterogenous Patient Responses to Healthcare Data Breach*, SSRN (Feb. 10, 2022), http://dx.doi.org/10.2139/ssrn.4029103. Under the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. §§1320d, *et seq.*, PHI is considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103. Health information such as diagnoses, treatment information, medical test results, and prescription information are considered PHI under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. Summary of the HIPAA Privacy Rule, U.S. Dep't of Health & Human Servs, https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Oct. 3, 2023).

12. Nuance breached its duty to Plaintiff and Class Members by maintaining Plaintiff's and the Class Members' Private Information in a negligent and reckless manner.

13. Upon information and belief, the means of the Data Breach and potential risk for improper disclosure of Plaintiff's and Class Members' Private Information were known and foreseeable to Nuance. Thus, Nuance was on notice that failing to take steps necessary to secure the Private Information from those risks left the Private Information in a dangerous and vulnerable condition.

14. Nuance and its employees failed to properly monitor the computer networks, databases, and systems housing the Private Information.

15. Had Nuance properly monitored its property and that of its third-party contractor, it would have discovered the intrusion sooner or been able to wholly prevent it.

16. Exacerbating an already devastating privacy intrusion, Plaintiff's and Class Members' identities are now at a heightened risk of exposure because of Nuance's negligent conduct since the Private Information that Nuance collected and stored is now in the hands of data thieves.

17. Armed with the Private Information accessed in the Data Breach, data thieves can now use the PII and PHI obtained from Nuance to commit a variety of crimes, including credit/debit card fraud, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' health information to target other phishing and hacking intrusions based upon their individual health needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class

Members' names but with another person's photograph, and giving false information to police during an arrest.

18. As a direct result of the Data Breach, Plaintiff and Class Members have suffered fraud and will continue to be exposed to a heightened and imminent risk of continuing fraud and identity theft, potentially for the rest of their lives. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

19. Plaintiff and Class Members may also incur out-of-pocket costs for purchasing credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft.

20. As a direct and proximate result of the Data Breach and subsequent exposure of their Private Information, Plaintiff and Class Members have suffered, and will continue to suffer damages and economic losses in the form of lost time needed to take appropriate measures to avoid unauthorized and fraudulent charges, putting alerts on their credit files, and dealing with spam phone calls, letters, and emails received as a result of the Data Breach.

21. Plaintiff and Class Members have suffered, and will continue to suffer, an invasion of their property interest in their own PII and PHI such that they are entitled to damages from Nuance for unauthorized access to, theft of, and misuse of their Private Information. These harms are ongoing, and Plaintiff and Class Members will suffer from future damages associated with the unauthorized use and misuse of their Private Information as thieves will continue to use the information to obtain money and credit in their names for several years.

22. Plaintiff seeks to remedy these harms on behalf of all similarly situated individuals whose Private Information was accessed via and/or compromised by Nuance during the Data Breach.

II. PARTIES

A. Plaintiff

23. Plaintiff Kristin Eyester ("Ms. Eyester") is a resident of Durham, North Carolina and a citizen of the State of North Carolina. Ms. Eyester learned of the Nuance Data Breach in October 2023. She was treated at WakeMed facilities in Durham and Raleigh, North Carolina.

B. Defendant

24. Defendant Nuance Communications, Inc. is a corporation organized under the laws of Delaware with its principal place of business in Redmond, Washington. Defendant maintains an office in Massachusetts at 1 Wayside Road, Burlington, MA. Nuance provides medical technology, including radiology imaging, utilized by WakeMed. which is part of the Duke University Health System.

III. JURISDICTION AND VENUE

25. This Court has subject-matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, consists of putative class membership of greater than 100 members, and is a class action in which some of the members of the Class, including Plaintiff, are citizens of states different than that of Defendant.

26. This Court has personal jurisdiction over Defendant because Defendant maintains an office in Massachusetts, frequently conducts business in Massachusetts, and has sufficient minimum contacts in Massachusetts.

27. Venue is proper in this Court pursuant to 28 U.S.C. §1391 because Defendant maintains an office in this District, a substantial part of the events, acts, and omissions giving rise

to Plaintiff's claims occurred in, was directed to, and/or emanated from this District, and Defendant conducts substantial business in this District.

IV. STATEMENT OF FACTS

A. Defendant Nuance's Business

28. Founded in 1992, Nuance touts itself as a "leading provider of conversational artificial intelligence ("AI") and cloud-based ambient clinical intelligence for healthcare providers."[2] A global company of over 7,100 employees, Nuance provides voice recognition technology, natural language processing, and clinical intelligence services to organizations across the healthcare, financial services, telecommunications, government, and retail sectors.[3] Nuance serves 77% of hospitals and 10,000 healthcare organizations worldwide, capturing "300 million patient stories each year."[4] Nuance operates in 28 countries and has a reported annual revenue of approximately $1.5 billion.[5]

29. Nuance's products and services include providing clinical documentation solutions for clinicians, radiologists, and care teams, as well as biometric security solutions facilitated by AI, advanced analytics, and machine learning algorithms.[6]

30. Specifically, Nuance provides medical voice recognition, medical imaging, transcription, and clinical documentation products to hospitals and medical providers. To deliver

[2] Nuance Communications, Inc. (Form 8-K) (Apr. 12, 2021).

[3] Nuance Communications, Inc. (Form 10-K) (Sept. 30, 2020).

[4] Healthcare AI Solutions & Services, Nuance Communications, Inc., https://www.nuance.com/healthcare.html (last visited Oct. 3, 2023).

[5] Nuance Communications, Inc. (Form 10-K) (Sept. 30, 2020).

[6] *Id.*

these products, Nuance collects patient data both directly from Nuance's healthcare customers as well as from vendors serving those healthcare customers directly, such as individual doctors, imaging and laboratory services providers, and electronic health record service providers. This patient data includes but is not limited to name, address, gender, birthdate, medical record number, diagnosis, image, and treatment information.[7]

31. In addition, Nuance offers its corporate customers voice recognition, text input, and communications products, requiring the collection and processing of personal data in those products, including voice recordings, text, names, phone numbers, or sensitive data such as credit card numbers, or unique identifier numbers issued on a government document commonly used to identify a person's identity.[8]

32. Nuance also provides biometric authentication products to corporate customers and collects, stores, and/or uses personal data processed in those products, including voiceprints, information regarding fingerprints, and information regarding behavior, for the purpose of confirming identity or detecting potentially fraudulent or malicious activity.[9]

B. The Collection of Plaintiff's and Class Members' Private Information is Central to Nuance's Business

33. In order for Nuance to offer its contracted services to healthcare provider clients, the healthcare provider clients were required to transfer possession of user PII and PHI to Nuance.

34. Through the possession and utilization of Plaintiff's and Class Members' Private Information, Nuance assumed duties owed to Plaintiff and Class Members regarding their Private

[7] Nuance Privacy Statement, Nuance Communications, Inc., https://www.nuance.com/about-us/company-policies/privacy-policies.html (last visited Oct. 3, 2023).

[8] *Id.*

[9] *Id.*

Information. Therefore, Nuance knew or should have known that it was responsible for safeguarding Plaintiff's and Class Members' Private Information from unauthorized access and criminal misuse.

35. Nuance has publicly touted its cybersecurity abilities, noting that "clients trust Nuance to deliver solutions that handle patient data responsibly."[10] Through Nuance's own Internal Code of Conduct, Nuance communicated that it has "an obligation to protect the privacy of the personal information [it] hold[s]."[11]

36. Indeed, in describing Nuance's stated implementation of de-identification and pseudonymization protocols, Nuance further emphasized its commitment to data privacy and protection:

> "An essential aspect of the benefits that we offer is our approach to processing personal information and sensitive or special category data. We believe it is critical to protect this information and to use it safely, securely, responsibly, and proportionally. At Nuance, we are committed to safeguarding the personal information and the data we hold. We employ sophisticated data handling methods to guard an individual's privacy while ensuring that the data remains useful for the purpose and support that people require."[12]

37. Nuance has also publicly touted its data risk management and risk reduction strategy. Through its "Data Governance Program," Nuance claims to manage the production, reliability, traceability, quality, integrity, disclosure, protection, and usage of data across the

[10] Global Privacy-Data Governance Program, Nuance Communications, Inc., https://www.nuance.com/about-us/trust-center/privacy/data-governance.html (last visited Oct. 3, 2023).

[11] Global compliance and ethics, Nuance Communications, Inc., https://www.nuance.com/about-us/trust-center/compliance.html (last visited Oct. 3, 2023).

[12] Global privacy—De-identification and pseudonymization, Nuance Communications, Inc., https://www.nuance.com/about-us/trust-center/privacy/de-identification-pseudonymization.html (last visited Oct. 3, 2023).

organization."[13] Through this program, Nuance undertook responsibility for prioritizing a range of data privacy practices, including data ownership and accountability, change management, standardized policies and procedures, consistent data quality management, data assessment and monitoring, and training and communications.[14]

38. Further, Nuance owed a duty to Plaintiff and Class Members to perform due diligence on the subcontractors and service vendors who receive Private Information from Nuance.

39. The circumstances of the Data Breach suggest that Nuance utterly failed to conduct sufficient due diligence on its subcontractor, Progress Software, whose file transfer application, MOVEit, was the conduit for the Data Breach.[15] This failure is demonstrated through Nuance's extensive use of vulnerable file transfer protocol software, and both Progress Software's delayed notification to Nuance of the vulnerability in its system and subsequent cyberattack, and the resulting breach of Plaintiff's and Class Members' PII and PHI.

40. Plaintiff and Class Members relied on Nuance to keep their Private Information secure and safeguarded for authorized purposes. Nuance owed a duty to Plaintiff to secure their Private Information as such, and ultimately breached that duty.

C. The Data Breach

41. On or around May 28, 2023, a cyber attacker targeted a "critical zero-day vulnerability" in the Progress Software file transfer application, MOVEit, utilized by Nuance for

---

[13] Global Privacy-Data Governance Program, Nuance Communications, Inc., https://www.nuance.com/about-us/trust-center/privacy/data-governance.html (last visited Oct. 3, 2023).

[14] *Id.*

[15] Notice of Progress Software Security Incident, Nuance Communications, Inc. https://www.nuance.com/moveit-support.html (last visited Oct. 3, 2023).

external file-sharing purposes.[16] The Russia-linked ransomware group CL0P has since claimed responsibility for the cyberattack.[17]

42. Through a post on its website and in Data Breach Notice templates filed with state attorneys general offices, Nuance provided further details on the Data Breach. On May 31, 2023, Progress Software informed Nuance of the Data Breach occurrence. Nuance states that it then launched an investigation. Over one month later, on July 11, 2023, Nuance confirmed that patient Private Information was compromised in the Data Breach. Upon information and belief, on August 1, 2023, Nuance began notifying healthcare entity clients of the Data Breach, but not underlying customers whose Private Information was compromised.

43. In the Notice Letter template, Nuance states that Plaintiff's and Class Members' PII and PHI had been exposed, and therefore compromised, in the attack, including:

i. Name;

ii. Date of Birth;

iii. Gender;

iv. Mailing Address;

v. Telephone Number;

vi. Email Address;

vii. Relative's Name

viii. Power of Attorney's Name

ix. Health Insurance Numbers;

---

[16] *Id.*

[17] *#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (June 7, 2023), https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

x. Dates of Service;

xi. Medical Facilities;

xii. Practitioners' Names;

xiii. Diagnostic Study Identifiers;

xiv. Clinical information such as treatments provided, medication information, diagnoses, diagnostic imaging reports; and

xv. Patient identifiers such as medical record numbers.

44. Over three months after the Data Breach, on or around September 15, 2023, Nuance began filing Notice templates with state attorneys general.

45. Nuance's Notice was untimely and woefully deficient, failing to provide basic details concerning the Data Breach, including, but not limited to, how unauthorized parties accessed the third-party MOVEit software, whether the information was encrypted or otherwise protected, whether the breach was a system-wide breach, and how many people were affected by the Data Breach.

46. Given the intentional and criminal nature of the cybersecurity attack, Plaintiff's and Class Members' Private Information is now for sale to criminals on the dark web; meaning unauthorized parties have accessed and viewed Plaintiff's and Class Members' unencrypted, unredacted Private Information, including names, dates of birth, billing and insurance information, medical records, diagnosis and prescription information, Social Security numbers, driver's licenses, and more.

D. Plaintiff's Experiences Following the Data Breach

Kristen Eyester

47. Plaintiff Eyestar is a patient of WakeMed Health & Hospitals. Prior to the Data Breach, she had medical care, including radiology services, at WakeMed's Durham and Raleigh facilities.

48. Prior to and during her medical appointments at WakeMed, Plaintiff Eyster provided her PII and PHI to WakeMed as a condition of receiving medical care.

49. After the Data Breach, the personal email account that held Plaintiff's financial and other sensitive data was fraudulently compromised. This is the same email account/email address that she provided to WakeMed during her medical appointments. Plaintiff Eyestar has discovered that a thief has taken over that email account and she no longer has access to it. Plaintiff Eyestar was forced to handle communications and data from a different email account and has since undertook the arduous process of changing her account passwords for just about all of her communications.

50. Ms. Eyestar is extremely concerned about how the theft of her email account is impacting all her other accounts and being a victim of identity theft as to her email account. Moreover, she is anxious because Defendant did not properly maintain the privacy of her Social Security Number, medical records, diagnosis and medical information, driver's license and additional data that she provided to WakeMed.

E. The Healthcare Sector Is Particularly Susceptible to Cyberattacks

51. Nuance was or should have been on notice that the Federal Bureau of Investigation ("FBI") has been concerned about data security in the healthcare sector. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare

industry that hackers were targeting them. The warning stated that "'[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII).'"[18]

52. The American Medical Association ("AMA") has also warned healthcare companies about the importance of protecting their patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[19]

53. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[20] In 2022, 1,802 data compromises were reported that impacted over 422 million victims—marking a 42% increase in the number of victims impacted since 2021.[21] That upward trend continues.

---

[18] Jim Finkle, *FBI warns healthcare firms that they are targeted by hackers*, REUTERS (Aug. 20, 2014), *available at* https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820 (last visited Oct. 3, 2023).

[19] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med. Ass'n (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals (last visited Oct. 3, 2023) (emphasis omitted).

[20] Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout, CISION PR Newswire (Jan. 19, 2017), https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html (last visited Oct. 3, 2023).

[21] 2022 Annual Data Breach Report, IDENTITY THEFT RES. CTR. (Jan. 2023), https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf (last visited Oct. 3, 2023).

54. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.[22] Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[23] Almost 50% of the victims lost their healthcare coverage as a result of the incident, while nearly thirty percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.[24]

55. Healthcare related data breaches also come at a cost to the breached entities. According to IBM's 2023 Cost of a Data Breach Report, the healthcare sector reported the highest data breach costs for the thirteenth year in a row in 2023—increasing 8.2% from $10.10 million in 2022 to $10.93 million in 2023.[25] This cost should only further incentivize service providers to both invest in and implement reasonable and adequate security measures in order to avoid financial repercussions in the event of a breach.

---

[22] 2018 End-of-Year Data Breach Report, IDENTITY THEFT RES. CTR. (2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINALWEB-V2-2.pdf (last visited Oct. 3, 2023).

[23] Elinor Mills, Study: Medical identity theft is costly for victims, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Oct. 3, 2023).

[24] *Id.*

[25] *See* Cost of a Data Breach Report, IBM.com, IBM, https://www.ibm.com/reports/data-breach (last visited Oct. 3, 2023).

56. Healthcare related data breaches have continued to rapidly increase. According to the 2019 HIMSS Cybersecurity Survey, 82% of participating hospital information security leaders reported having a significant security incident in the last 12 months, with a majority of these known incidents being caused by "bad actors" such as cybercriminals.[26]

> Hospitals have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information (PII) for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.[27]

57. Given Nuance's work centered on accessing and maintaining sensitive PII and PHI, Nuance knew or reasonably should have known the importance of implementing reasonable and adequate practices and procedures in order to safeguard the PII and PHI entrusted to it by individuals receiving healthcare services.

58. As entities both contracting with healthcare service providers and handling, storing, and safeguarding PII and PHI, Nuance knew, or reasonably should have known, the importance of safeguarding the Private Information entrusted to it, and of the foreseeable consequences if its data security systems were breached. This duty extends to Nuance's obligations to safeguard PII and PHI shared with subcontractors and service vendors who received Private Information from Nuance. Nuance failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

---

[26] 2019 HIMSS Cybersecurity Survey, HIMSS, https://www.himss.org/sites/hde/files/d7/u132196/2019_HIMSS_Cybersecurity_Survey_Final_Report.pdf (last visited Oct. 3, 2023).

[27] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, CHIEF HEALTHCARE EXEC. (Apr. 4, 2019), https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks.

F. The Value of Private Information and the Effects of Unauthorized Disclosure

59. At all relevant times, Nuance was well aware that the Private Information it collects from Plaintiff and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

60. Private Information is a valuable commodity to cyber attackers. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and medical and financial fraud.[28] Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground websites, commonly referred to as the dark web.

61. While credit card information and associated PII can sell for as little as $1-$2 on the black market, PHI can sell for as much as $363.[29]

62. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

63. Medical identify theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "'Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery,'"

---

[28] *What to Know About Identify Theft*, Fed. Trade Comm'n, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Oct. 3, 2023).

[29] *Data Breaches: In the Healthcare Sector,* Ctr. for Internet Sec., https://www.cisecurity.org/blog/data-breaches-in-the-healthcare-sector/ (last visited Oct. 3, 2023).

reported Pam Dixon, executive director of World Privacy Forum. "'Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities.'"[30]

64. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. EHR can then be used to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. EHR theft is also more difficult to detect, taking almost twice as long as normal identity theft.[31]

65. The ramifications of Nuance's failures to keep Plaintiff's and Class Members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to twelve months or even longer.

66. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

67. Approximately 21% of victims do not realize their identity has been compromised until more than two years after it has happened.[32] This gives thieves ample time to seek multiple treatments under the victim's name. And 40% of consumers found out they were a victim of

---

[30] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, Kaiser Health News (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.

[31] *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI CYBER DIV. (Apr. 8, 2014), https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf.

[32] *See Medical ID Theft Checklist*, IdentityForce https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Oct. 3, 2023).

medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[33]

68. As a company contracting with healthcare entities, Nuance knew, or reasonably should have known, the importance of safeguarding Plaintiff's and Class Members' Private Information entrusted to it, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach. Nuance failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

G. Nuance's Conduct Violates HIPAA

69. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of PHI. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.[34]

70. Nuance is a covered entity under HIPAA and is therefore required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

---

[33] *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages*"), Experian (Apr. 2010), https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[34] *What is Considered Protected Health Information Under HIPAA?*, HIPAA J. (Jan. 1, 2023), https://www.hipaajournal.com/what-is-considered-protected-health-information-under-hipaa/.

71. Title II of HIPAA contains the Administrative Simplification provisions. 42 U.S.C. §§1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Nuance failed to safeguard. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

72. The HIPAA Breach Notification Rule, 45 CFR §§164.400-414, also required Nuance to provide notice of the breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of a breach."[35]

73. Based on information and belief, Nuance's Data Breach resulted from a combination of insufficiencies that demonstrate Nuance failed to comply with safeguards mandated by HIPAA regulations and industry standards. Nuance's security failures include, but are not limited to, the following:

a. Failing to ensure the confidentiality and integrity of electronic protected health information that Nuance receives, maintains, and transmits in violation of 45 C.F.R. §164.306(a)(1);

b. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. §164.312(a)(1);

c. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. §164.308(a)(1);

d. Failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. §164.308(a)(6)(ii);

[35] *Breach Notification Rule*, U.S. Dep't of Health & Human Servs., https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Oct. 3, 2023) (emphasis added).

e. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 C.F.R. §164.306(a)(2);

f. Failing to protect against any reasonably anticipated uses or disclosures of electronically protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. §164.306(a)(3);

g. Failing to ensure compliance with HIPAA security standard rules by its workforce in violation of 45 C.F.R. §164.306(a)(94);

h. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 C.F.R. §164.502, *et seq.*;

i. Failing to effectively train all members of its workforce (including independent contractors) on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of protected health information in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §164.308(a)(5); and

j. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard protected health information, in compliance with 45 C.F.R. §164.530(c).

H. Nuance Failed to Comply with FTC Guidelines

74. Nuance was also prohibited by the Federal Trade Commission Act ("FTCA") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA.[36]

[36] *See, e.g.*, *In re Cap. One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020) (citing *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015)).

75. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[37]

76. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[38] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.

77. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

78. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. §45. Orders resulting from these actions further clarify the measures businesses must take to meet its data security obligations.

---

[37] *Start With Security: A Guide for Business*, Fed. Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Oct. 3, 2023).

[38] *Protecting Personal Information: A Guide for Business*, Fed. Trade Comm'n (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Oct. 3, 2023).

79. Nuance failed to properly implement basic data security practices. Nuance's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. §45.

80. Nuance was fully aware of its obligations to protect the Private Information of Plaintiff and Class Members because of its position as a service provider whose business centers on the collection, storage, and safeguarding of PII and PHI. Nuance was also aware of the significant repercussions that would result from its failure to make good on those obligations.

I. Cyber Criminals Have and Will Continue to Use Plaintiff's and Class Members' PII and PHI for Nefarious Purposes

81. Plaintiff's and Class Members' highly sensitive PII and PHI is of great value to cybercriminals, and the data stolen in the Data Breach can be used in a variety of ways for criminals to exploit Plaintiff and the Class Members and to profit off their misfortune and stolen information. The cybercriminals' motives for the Data Breach were purely nefarious and malicious in nature: their one goal was to access systems, including Nuance's systems, in order to obtain valuable PII and PHI to sell on the dark web.

82. Every year, identity theft causes tens of billions of dollars of losses to victims in the United States.[39] For example, with the PII stolen in the Data Breach, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and

[39] *Facts + Statistics: Identity Theft and Cybercrime*, Ins. Info. Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (last visited Oct. 3, 2023) (discussing Javelin Strategy & Research's report *2018 Identity Fraud: Fraud Enters a New Era of Complexity*).

many other harmful forms of identity theft.[40] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

83. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.

84. These risks are both certainly impending and substantial. As the FTC has reported, if cyber attackers get access to PII, they will use it.[41]

85. Cyber attackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[42]

86. If cyber criminals manage to access PII, health insurance information, and other personally sensitive data, as is the case with this Data Breach, there is no limit to the amount of fraud to which Nuance may have exposed Plaintiff and Class Members.

J. Plaintiff and Class Members Suffered Damages

87. The ramifications of Nuance's failures to keep Plaintiff's and Class Members' Private Information secure are long lasting and severe. Once Private Information is stolen,

---

[40] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, USA Today (Nov. 15, 2017), https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity-thief-can-use-your-social-security-number/860643001/ (last visited Oct. 3, 2023).

[41] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737, Government Accountability Office (Jul. 5, 2007), https://www.gao.gov/assets/a262904.html (last visited Oct. 3, 2023).

[42] Stolen Laptops Lead to Important HIPAA Settlements, U.S. DEP'T OF HEALTH & HUMAN SERVS. (Apr. 22, 2014), https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[43]

88. In addition to their obligations under state laws and regulations, Nuance owed – and directly undertook the common law duty to Plaintiff and Class Members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties. This duty extends to Nuance's obligations to safeguard PII and PHI shared with subcontractors and service vendors who received Private Information from Nuance, and to conduct ongoing, robust due diligence into such subcontractors and service vendors prior to contracting and throughout any relationship.

89. Nuance further owed and breached its duties to Plaintiff and Class Members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems. Instead of implementing such processes and specifications, Nuance allowed the Data Breach to go undetected for three days before it was alerted by its third-party vendor of the cyberattack.

90. As a direct result of Nuance's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, cyber attackers were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiff's and Class Members' Private Information as detailed above, and Plaintiff is now at a heightened risk of identity theft and fraud.

[43] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

91. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

92. Other risks of identity theft include loans opened in the name of the victim, medical services billed in their name, utility bills opened in their name, tax return fraud, and credit card fraud.

93. Plaintiff and Class Members did not receive the full benefit of the bargain for received healthcare and other services. As a result, Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value of the healthcare services with data security protection they paid for and the services they received without the data security protection.

94. As a result of the Data Breach, Plaintiff's and Class Members' Private Information has lost potential value.

95. The Private Information belonging to Plaintiff and Class Members is private, private in nature, and was left inadequately protected by Nuance who did not obtain Plaintiff's or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

96. The Data Breach was a direct and proximate result of Nuance's failure to: (a) properly safeguard and protect Plaintiff's and Class Members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative,

technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

97. Nuance had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect patient data.

98. Had Nuance remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into their systems and, ultimately, the theft of Plaintiff's and Class Members' Private Information.

99. As a direct and proximate result of Nuance's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

100. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "[r]esolving the problems caused by identity theft [could] take more than a year for some victims."[44]

101. Nuance's failures to adequately protect Plaintiff's and Class Members' Private Information has resulted in Plaintiff and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services,

[44] Erika Harrell, & Lynn Langton, *Victims of Identity Theft, 2012*, U.S. Dep't of Just., Off. of Just. Programs Bureau of Just. Stats. (Dec. 2013), https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited Oct. 3, 2023).

payment of money. Rather than assist those affected by the Data Breach, Nuance is putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

102. As a result of Nuance's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Private Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fail to undertake appropriate measures to protect the Private Information in their possession;

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and

f. Anxiety and distress resulting from fear of misuse of their medical information.

103. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their Private Information is secure, remains secure, and is not subject to further misappropriation and theft.

K. Nuance's Delay in Identifying & Reporting the Breach Caused Additional Harm

104. It is axiomatic that:

> "[t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred

> on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[45]

105. Indeed, once a data breach has occurred,

> "[o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers.
>
> "If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves . . . . "[46]

106. Although their Private Information was improperly exposed on or before May 28, 2023, Nuance did not notify Plaintiff and Class Members until over three months following the Data Breach. Nuance's delay deprived Plaintiff and Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

107. As a result of Nuance's delay in detecting and notifying individuals of the Data Breach, the risk of fraud for Plaintiff and Class Members has been driven even higher.

CLASS ALLEGATIONS

108. Plaintiff brings this class action on behalf of herself and all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

109. The Class that Plaintiff seeks to represent is defined as follows:

> **All individuals in the United States whose Private Information was compromised in the Nuance Data Breach.**

---

[45] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire (Feb. 1, 2017), https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million (last visited Oct. 3, 2023).

[46] Allen St. John, *The Data Breach Next Door*, Consumer Reports, (Jan. 31, 2019), https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last visited Oct. 3, 2023).

110. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

111. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

112. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members is impracticable. Defendant has identified at least 1.2 million individuals whose Private Information may have been improperly accessed and compromised in the Data Breach.

113. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and when Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining Class Members' Private Information;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class Members' Private Information;

e. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class Members' Private Information;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' Private Information secure and prevent loss or misuse of that Private Information;

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiff's and Class Members' damages;

i. Whether Defendant violated the law by failing to promptly notify Class Members that their Private Information had been compromised;

j. Whether Plaintiff and the other Class Members are entitled to actual damages, extended credit monitoring, and other monetary relief;

k. Whether Defendant violated common law and statutory claims alleged herein.

114. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members, because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

115. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect the Class uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

116. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel

experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

117. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

118. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of the Class with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

119. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

120. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

121. Unless a Class-wide injunction is issued, Plaintiff and Class Members remain at risk that Defendant will continue to fail to properly secure the Private Information of Plaintiff and Class Members resulting in another data breach, continue to refuse to provide proper notification to Class Members regarding the Data Breach, and continue to act unlawfully as set forth in this Class Action Complaint.

122. Defendant acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

123. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to the following:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable and adequate security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Class Members are entitled to actual damages, additional credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

124. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

125. Plaintiff and Class Members were required to submit their Private Information in order to receive healthcare services.

126. Defendant knew, or should have known, of the risks inherent in collecting and storing the Private Information of Plaintiff and Class Members.

127. As described above, Defendant owed a duty of care to Plaintiff and Class Members whose Private Information had been entrusted with Defendant.

128. Defendant breached its duty to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

129. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' Private Information. Defendant knew or reasonably should have known that it had inadequate data security practices to safeguard such information, and Defendant knew or reasonably should have known that data thieves were attempting to access databases containing PII and PHI, such as those of Defendant.

130. A "special relationship" exists between Defendant and Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members

because Defendant collected the Private Information of Plaintiff and the Class Members—information that Plaintiff and the Class Members were required to provide in order to receive healthcare services.

131. But for Defendant's wrongful and negligent breach of the duty owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

132. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breaches of its duty. Defendant knew or reasonably should have known it was failing to meet its duty, and that Defendant's breach of such duty would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

133. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

134. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

135. Defendant accepted the special confidence placed in it by Plaintiff and Class Members, asserting that it is "committed to safeguarding the personal information and the data [it] hold[s]." There was an understanding between the parties that Defendant would act for the benefit of Plaintiff and Class Members in preserving the confidentiality of the Private Information.

136. Defendant became the guardian of Plaintiff's and Class Members' Private Information and accepted a fiduciary duty to act primarily for the benefit of those by storing and safeguarding their Private Information.

137. Defendant breaches its fiduciary duties to Plaintiff and Class Members by failing to: (a) diligently discover, investigate, or give notice of the Data Breach in a reasonable and practicable period of time; (b) encrypt and otherwise protect the integrity of its computer systems containing Plaintiff's and the Class Members Private Information; (c) timely notify and/or warn them of the Data Breach; (d) ensure the confidentiality and integrity of electronic PHI Defendant received, maintained, and transmitted in violation of 45 C.F.R. §164.306(a)(1); (e) implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. §164.312(a)(1); (f) implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. §164.308(a)(1); (g) identify and respond to suspected or known security incidents and to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. §164.308(a)(6)(ii); (h) protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI, in violation of 45 C.F.R. §164.306(a)(2); (i) protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. §164.306(a)(3); (j) ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 C.F.R. §164.306(a)(94); (k) effectively train all members of its workforce (including independent contractors) on the policies and procedures necessary to maintain the security of PHI, in violation of 45 C.F.R. §164.530(b) and 45 C.F.R. §64.308(a)(5); (l) design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in violation of 45 C.F.R. §164.530(c); and (m) by otherwise failing to safeguard Plaintiff's and the Class Members' Private Information.

138. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

139. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

140. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

141. Plaintiff and Class Members entered into an implied contract with Defendant when they sought or obtained services from their respective healthcare providers, in exchange for which

they were required to provide their Private Information. The Private Information provided by Plaintiff and Class Members to Defendants was governed by and subject to Defendant's privacy duties and policies.

142. Defendant agreed to safeguard and protect the Private Information of Plaintiff and Class Members and to timely and accurately notify Plaintiff and Class Members in the event that their Private Information was breached or otherwise compromised.

143. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class Members believed that Defendant would use part of the monies paid to Defendant under the implied contracts to fund adequate and reasonable data security practices.

144. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract or implied terms between Plaintiff and Class Members and Defendant. The safeguarding of the Private Information of Plaintiff and Class Members and prompt and sufficient notification of a breach involving Private Information was critical to realize the intent of the parties.

145. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

146. Defendant breached its implied contracts with Plaintiff and Class Members to protect Plaintiff's and Class Members' Private Information when it: (1) failed to have data security practices in place to protect that information; (2) failed in performing appropriate due diligence of third-party contractors handling patients' Private Information; (3) disclosed that information to

unauthorized third parties; and (4) failed to provide timely and accurate notice that their Private Information was compromised as a result of the Data Breach.

147. As a direct and proximate result of Defendant's breaches of implied contract, Plaintiff and Class Members have suffered damages.

PRAYER FOR RELIEF

A. That the Court certify this action as a class action and certify the Class as proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is the proper class representative; and appoint Plaintiff's Counsel as Class counsel;

B. That the Court grant permanent injunctive relief to prohibit Defendant from engaging in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and members of the Class compensatory, consequential, and general damages in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of its unlawful acts, omissions, and practices;

E. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

F. That Plaintiff be granted the declaratory relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. That the Court award pre- and post-judgment interest at the maximum legal rate; and

I. That the Court grant all such other relief as it deems just and proper.

Dated: October 3, 2023

Respectfully submitted,

BERMAN TABACCO

/s/ Patrick T. Egan

Patrick T. Egan (BBO #637477)
Nathaniel L. Orenstein (BBO #664513)
Christina L. Gregg (BBO #709220)
One Liberty Square
Boston, MA 02109
Telephone: (617) 542-8300
pegan@bermantabacco.com
norenstein@bermantabacco.com
cgregg@bermantabacco.com

Lori G. Feldman, Esq.
GEORGE GESTEN MCDONALD, PLLC
102 Half Moon Bay Drive
Croton-on-Hudson, NY 10520
Telephone: (561) 232-6002
Facsimile: (888) 421-4173
lfeldman@4-justice.com
E-Service: eService@4-justice.com

CERTIFICATE OF SERVICE

I hereby certify that on October 3, 2023 a copy of the foregoing was filed electronically. Service of this filing will be made on all ECF-registered counsel by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/ Patrick T. Egan